A FREE CHECKLIST FROM TAGGERUNG SOLUTIONS

The December scam checklist

Five messages that show up at small companies this time of year, the one habit that stops most of them, and what to do if money already went out. Print it for whoever pays your bills.

The one rule: call back on the number you already have

Before money moves to new bank details, or because a message says it's urgent, call the person on a number you had before this message arrived. Not the number in the email, the text or the new invoice.

FIVE MESSAGES WORTH A SECOND LOOK

1 **An invoice from a vendor you really use**

Real logo, real job, an amount that matches a delivery. Someone may be inside the vendor's email, so it can look exactly like the last ten.

Do this: Compare the bank details to the last invoice you paid. If anything changed, call before you pay.

2 **"We changed banks, please use this account"**

Usually lands right before a big payment, often with a reason it has to happen today.

Do this: Never change bank details from an email. Call the number on file, and have a second person confirm the change.

3 **A text from "the boss" asking for gift cards**

"I'm in a meeting, can you grab a few gift cards for a customer? I'll pay you back." Aimed at whoever wants to help.

Do this: Nobody at your company asks for gift cards by text. Call the boss on the number you already have.

4 A delivery problem with a link to fix it

A missed package, a customs fee, an address to confirm. December is full of real deliveries, so these blend in.

Do this: Don’t tap the link. Open the carrier’s app or type their website in yourself and look up the tracking number.

5 A call or pop-up saying your account is locked

“This is Microsoft” or “This is Google, your business listing will be suspended.” They want a payment, a code, or remote access.

Do this: Hang up. Don’t call back the number they gave. Read out a sign-in code to no one, ever.

SET IT UP ONCE

Ten minutes that cover the whole year

Each of these is a decision or a setting, not software. Tick them off with whoever handles payments.

- [ ] Pick a dollar amount for two approvals. Above it, a second person signs off before money moves. Choose a number that fits your company.
- [ ] Send your vendors the one-page letter on the next page, so everyone knows bank changes never happen by email.
- [ ] Turn on two-step sign-in for email, the bank and your accounting software. A stolen password alone then gets nobody in.
- [ ] Keep a phone list you trust for your top vendors and subs, written down before anyone needs it.
- [ ] Say the rules out loud once. A morning meeting or a staff text: no gift cards by text, and anything about money gets a phone call first.
- [ ] Know who you’d call. Your bank’s fraud line, and whoever looks after your computers and email.

IF MONEY ALREADY WENT OUT

Speed matters more than embarrassment. Do these the same hour, not Monday.

1. Call your bank's fraud line and ask them to recall or stop the payment. The sooner they hear, the better the odds.
2. Change the email password of whoever received the message, and check that mailbox for forwarding rules nobody set up on purpose.
3. Report it to the FBI at ic3.gov. Your bank may ask for the report number.
4. Tell your insurance agent if you carry cyber or crime coverage. Many policies want to hear about it quickly.
5. Warn the real vendor, on the number you already had. Their email may be the one that was taken over.

COPY AND SEND

A one-page letter for your vendors

Fill in the brackets and send it to every vendor and sub you pay.

Hello,

To protect both of us from payment fraud, [Company name] will never change where we send payments because of an email, a text or a new invoice. That includes requests that look like they come from your company.

If your bank details change, please call [name] at [phone number] and we'll confirm the change with you by phone before any payment goes to the new account.

If you ever get a message that appears to come from us asking you to pay a new account, please call us at the same number before you act on it.

[Your name]
[Company name]

Most of this needs a habit, not software. If you'd like a second set of eyes on how payments get approved or how your email is set up, I do a free 30-minute look.

Andrew Allen, Taggerung Solutions · taggerungsolutions.com

FOR THE OFFICE WALL · [COMPANY NAME]

Our rules about money

1. We never change where we send money because of an email or a text.
2. New bank details get a call to a number we already had.
3. Payments over $[amount] need a second person to approve.
4. Nobody here asks for gift cards by text. Ever.
5. We don’t tap links about deliveries or locked accounts. We look it up ourselves.
6. If something feels off, call [name] at [phone]. You won’t get in trouble for asking.